UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/839,551	04/19/2001	Stephen F. Bisbee	003670-074	1293

7590 06/04/2004

Michael G. Savage, Esquire
BURNS, DOANE, SWECKER & MATHIS, L.L.P.
P.O. Box 1404
Alexandria, VA 22313-1404

EXAMINER	
FLEURANTIN, JEAN B	
ART UNIT	**PAPER NUMBER**
2172	5

DATE MAILED: 06/04/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/839,551	BISBEE ET AL.	
	Examiner	Art Unit	
	Jean B Fleurantin	2172	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 August 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-41* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-41* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *3*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This is in response to the amendment filed 25 August 2003, in which claims 1-41 remain pending for examination.

Information Disclosure Statement

2. The information disclosure statement (IDS) file on 08/25/03 (Paper No. 3) complies with the provisions of M.P.E.P. 609. It has been placed in the application file. The information referred to therein has been considered as to merits. (See attached form).

Response to Applicant' Remarks

3. Applicant's arguments with respect to claims 1-41 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-5, 10-17, 29-32 and 37-41 are rejected under 35 U.S.C. 102(b) as being anticipated by US Pat. No. 5,999,711 (hereinafter "Misra").

As per claims 1, Misra discloses, "a method of enabling access to a resource of a processing system" (see col. 1, line 49 to col. 2, line 21), comprising the steps of:

"establishing a secure communication session between a user desiring access and a logon component of the processing system", (see col. 1, line 60 to 2, line 3);

"verifying that logon information, provided by the user to the logon component during the secure communication session, matches stored information identifying the user to the processing system", (see col. 1, line 66 to 2, line 4);

"generating a security context from the logon information and authorization information that is necessary for access to the resource", (see col. 1, line 50-55);

"providing the security context to the user", (see col. 1, lines 55-62); and

"sending, by the user to the processing system, the security context and a request for access to the resource", (see col. 1, line 60 to col. 2, line 3).

As per claims 2 and 16, Misra discloses, "wherein the resource is at least one of a processor, a program object, and a record of the processing system", (see col. 4, lines 30-35).

As per claim 3, Misra discloses, "wherein the logon component provides a symmetric encryption key to the user in establishing the secure communication session", (see col. 7, lines 35-44).

As per claims 4 and 31, Misra discloses, "wherein the logon information includes a password and at least one of a user identifier, an organization identifier, a sub-organization identifier, a user location, a user role, and a user position", (see col. 5, lines 45-55).

As per claims 5 and 32, Misra discloses, "wherein the logon information is verified by checking for agreement between the stored information identifying the user to the processing system and the password and at least one of a user identifier, an organization identifier, a sub-organization identifier, a user location, a user role, and a user position provided by the user to the logon component", (see col. , lines 35-45).

As per claims 10 and 37, Misra further discloses, "the step of determining, by a stateless component of the processing system, based on the security context sent with the request for access by the user, whether access to the requested resource should be granted to the user" as the authorization database holds no information about the user, (see col. 9, lines 20-35).

As per claims 11 and 38, Misra discloses, "wherein the communication device at least partially encrypts the request for access with a symmetric encryption key included in the security context", (see col. 6, lines 15-20).

As per claims 12 and 39, Misra discloses, "wherein a hash value is computed over the request for access, the hash value is included with the security context and the request for access sent by the user to the processing system, the integrity of the request for access is checked based

on the hash value, and access is granted only if the integrity of the hash value is verified", (see col. 6, lines 1-15).

As per claims 13 and 40, Misra discloses, "wherein the user digitally signs the request for access, the user's digital signature is included with the security context and the request for access sent by the user to the processing system, the user's digital signature is checked by the processing system, and access to the resource is granted only if the user's digital signature is authenticated" (see col. 9, lines 15-40).

As per claim 14, Misra discloses, "wherein the request for access comprises a wrapper", (see col. 1, lines 49-60).

As per claim 15, Misra further discloses, "the step, after access to the requested resource is granted, of sending a response to the user that includes a request counter that enables the user to match the response to the request for access", (see col. 5, lines 46-54).

As per claim 17, Misra discloses, "wherein the user sends the request counter and access to the resource is denied if the request counter differs from a predetermined value", (see col. 2, lines 8-29).

As per claim 29, Misra discloses, "a processing system having resources that are selectively accessible to users, the resources including processors, program objects, and records" (see col. 4, lines 30-40), the processing system comprising:

"a communication device through which a user desiring access to a resource communicates sends and receives information in a secure communication session with the processing system", (see col. 4, lines 20-30), and column 7, lines 20-25;

"an information database that stores information identifying users to the processing system and authorization information that identifies resources accessible to users and that is necessary for access to resources" (see col. 7, lines 50-55); and

"a logon component that communicates with the communication device and with the information database, wherein the logon component receives logon information provided by the user during the secure communication session, verifies the received logon information by matching against information identifying the user to the processing system that is retrieved from the information database, and generates a security context from the received logon information and authorization information" (see col. 8, lines 35-65);

"wherein the logon component provides the security context to the user's communication device, and the user sends, to the processing system, the security context and a request for access to a resource", (see col. 8, line 65 to col. 9, line 10).

As per claim 30, Misra further discloses, "a cryptographic accelerator, and wherein the logon component receives a symmetric encryption key from the cryptographic accelerator and

provides the symmetric encryption key to the user's communication device", (see col. 7, lines 35-44).

As per claim 41, the limitations of claim 41 are rejected in the analysis of claim 1, and this claim is rejected on that basis.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 6-9, 18-28 and 33-36 are rejected under U.S.C. 103(a) as being unpatentable over US Pat. No. 5,999,711 issued to Misra et al. (hereinafter "Misra") in view of "Probable Plaintext Cryptanalysis of the IP Security Protocols" – Steven M. Bellovin – 1997 (hereinafter "Bellovin").

As per claims 6 and 33, in addition to claim 1, Misra does explicitly discloses a plaintext header. However, Bellovin discloses a system wherein the encryption of plaintext and decryption, (see Bellovin, page 52, col. 2, paragraph 6 to page 53, paragraph 5). It would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify

the combined teachings of Misra and Bellovin with plaintext header. Such modification would allow the teachings of Misra and Bellovin to improve the accuracy and the reliability of the systems and method for state less authentication.

As per claims 7 and 34, Misra discloses, "wherein the encrypted body comprises at least one of a user identifier, an organization identifier, access information, an expiration time, public key information, symmetric key information, and a hash", (see figure 2A, col. 9, lines 45-55).

As per claims 8 and 35, Misra discloses, "wherein the access information specifies at least one resource accessible by the user; the expiration time specifies a time after which the security context is invalid; the hash is computed over the plaintext header and the encrypted body before encryption; and the hash is digitally signed by the logon component", (see col. 9, lines 45-55).

As per claims 9 and 36, Misra discloses, "wherein the encrypted body includes the expiration time and access to the resource is denied if the expiration time differs from a selected time", (see col. 9, lines 45-60).

As per claim 18, in addition to claim 1, Misra further discloses, "determining, by a stateless component of the processing system, based on the security context sent with the request for access by the user, whether access to the requested resource should be granted to the user", (col. 9, lines 20-35). Misra does not explicitly disclose wherein the security context comprises a

plaintext header. However, Bellovin discloses a system wherein the encryption of plaintext and decryption, (see Bellovin, page 52, col. 2, paragraph 6 to page 53, paragraph 5). It would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the combined teachings of Misra and Bellovin with plaintext header. Such modification would allow the teachings of Misra and Bellovin to improve the accuracy of the systems and method for state less authentication.

As per claim 19, Misra discloses, "wherein the security context includes a symmetric encryption key, and the request for access is at least partially encrypted with the symmetric encryption key", (see col. 7, lines 35-44).

As per claim 20, Misra discloses, "wherein the logon information includes a password and at least one of a user identifier, an organization identifier, a sub-organization identifier, a user location, a user role, and a user position", (see col. 5, lines 45-55).

As per claim 21, Misra discloses, "wherein the logon information is verified by checking for agreement between the stored information identifying the user to the processing system and the password and at least one of a user identifier, an organization identifier, a sub-organization identifier, a user location, a user role, and a user position provided by the user to the logon component", (see col. 8, lines 35-45).

As per claim 22, Misra discloses, "wherein the access information specifies at least one resource accessible by the user; the expiration time specifies a time after which the security context is invalid; the hash is computed over the plaintext header and the encrypted body before encryption; and the hash is digitally signed by the logon component", (see col. 8, lines 35-45).

As per claim 23, Misra discloses, "wherein the encrypted body includes the expiration time and access to the resource is denied if the expiration time differs from a selected time", (see col. 5, lines 45-60).

As per claim 24, Misra discloses, "wherein a hash value is computed over the request for access, the hash value is included with the security context and the request for access sent by the user to the processing system, the integrity of the request for access is checked based on the hash value, and access is granted only if the integrity of the hash value is verified", (see col. 6, lines 1-15).

As per claim 25, Misra discloses, "wherein the user digitally signs the request for access, at least the user's digital signature and the request for access are enclosed in a wrapper, the security context and the wrapper are sent to the processing system, the user's digital signature is checked by the processing system, and access to the resource is granted only if the user's digital signature is authenticated", (see col. 9, lines 15-40).

As per claim 26, Misra further discloses, "after access to the requested resource is granted, of sending a response to the user that includes a request counter that enables the user to match the response to the request for access", (see col. 5, lines 46-54).

As per claim 27, Misra discloses, "wherein at least one of a client time and a request counter is sent by the user to the processing system with the security context and the request for access to the resource", (see col. 5, lines 46-54).

As per claim 28, Misra discloses, "wherein the request counter is sent by the user and access to the resource is denied if the request counter differs from a predetermined value", (see col. 5, lines 45-60).

Prior Art

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

US 5,719,941 issued to Swift et al.

US 6,192,361 issued to Huang

US 6,581,060 issued to Choy

CONTACT INFORMATION

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jean B Fleurantin whose telephone number is 703-308-6718. The examiner can normally be reached on 7:30-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John B Breene can be reached on 703-305-9790. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jean Bolte Fleurantin

SHAHID ALAM
PRIMARY EXAMINER

May 16, 2004